FIG.1

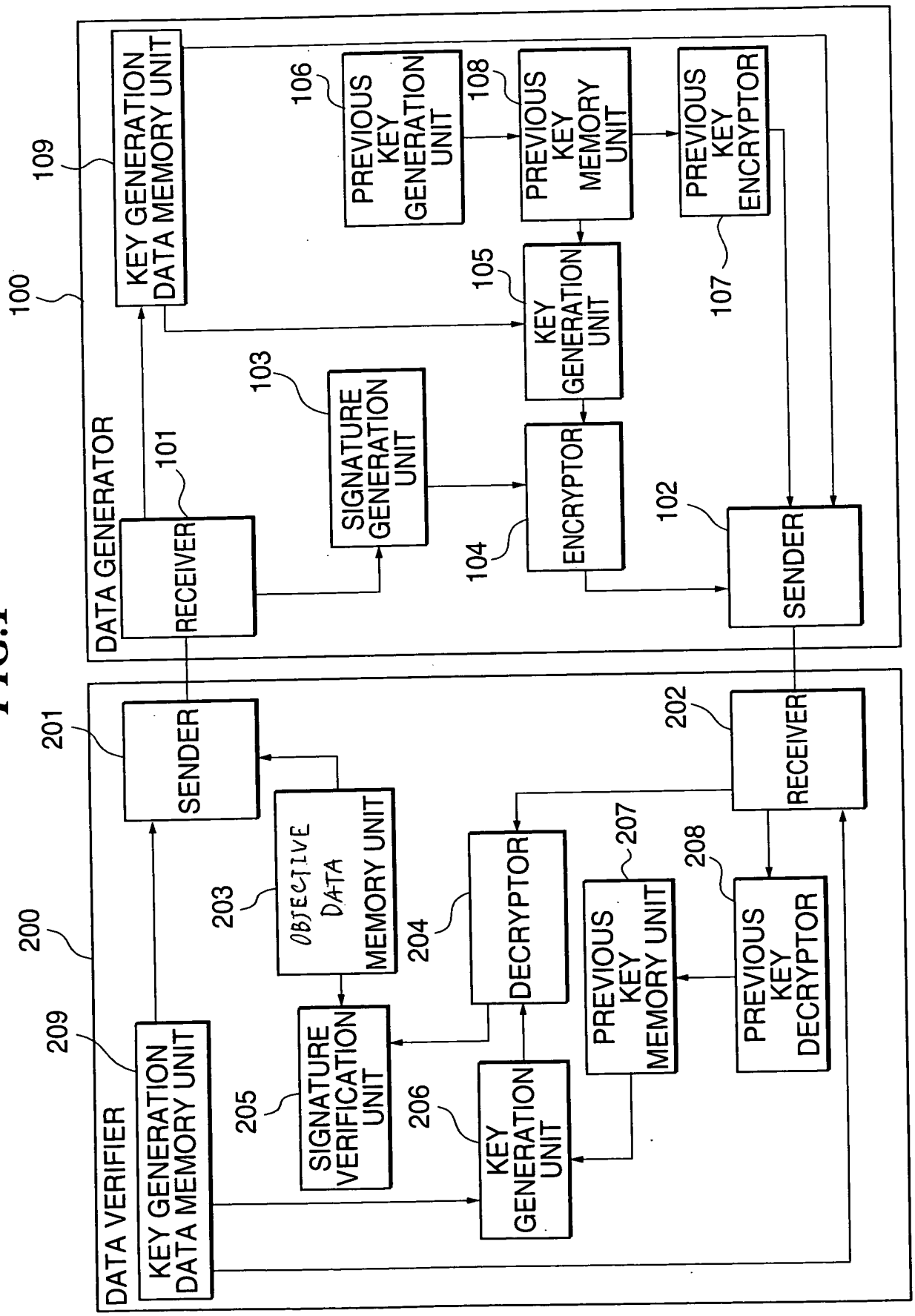

DATA GENERATOR
100
KEY GENERATION DATA MEMORY UNIT
109
RECEIVER
101
SIGNATURE GENERATION UNIT
103
ENCRYPTOR
104
SENDER
102
KEY GENERATION UNIT
105
PREVIOUS KEY GENERATION UNIT
106
PREVIOUS KEY MEMORY UNIT
108
PREVIOUS KEY ENCRYPTOR
107
DATA VERIFIER
200
KEY GENERATION DATA MEMORY UNIT
209
SENDER
201
OBJECTIVE DATA MEMORY UNIT
203
SIGNATURE VERIFICATION UNIT
205
DECRYPTOR
204
KEY GENERATION UNIT
206
PREVIOUS KEY MEMORY UNIT
207
PREVIOUS KEY DECRYPTOR
208
RECEIVER
202

FIG.2

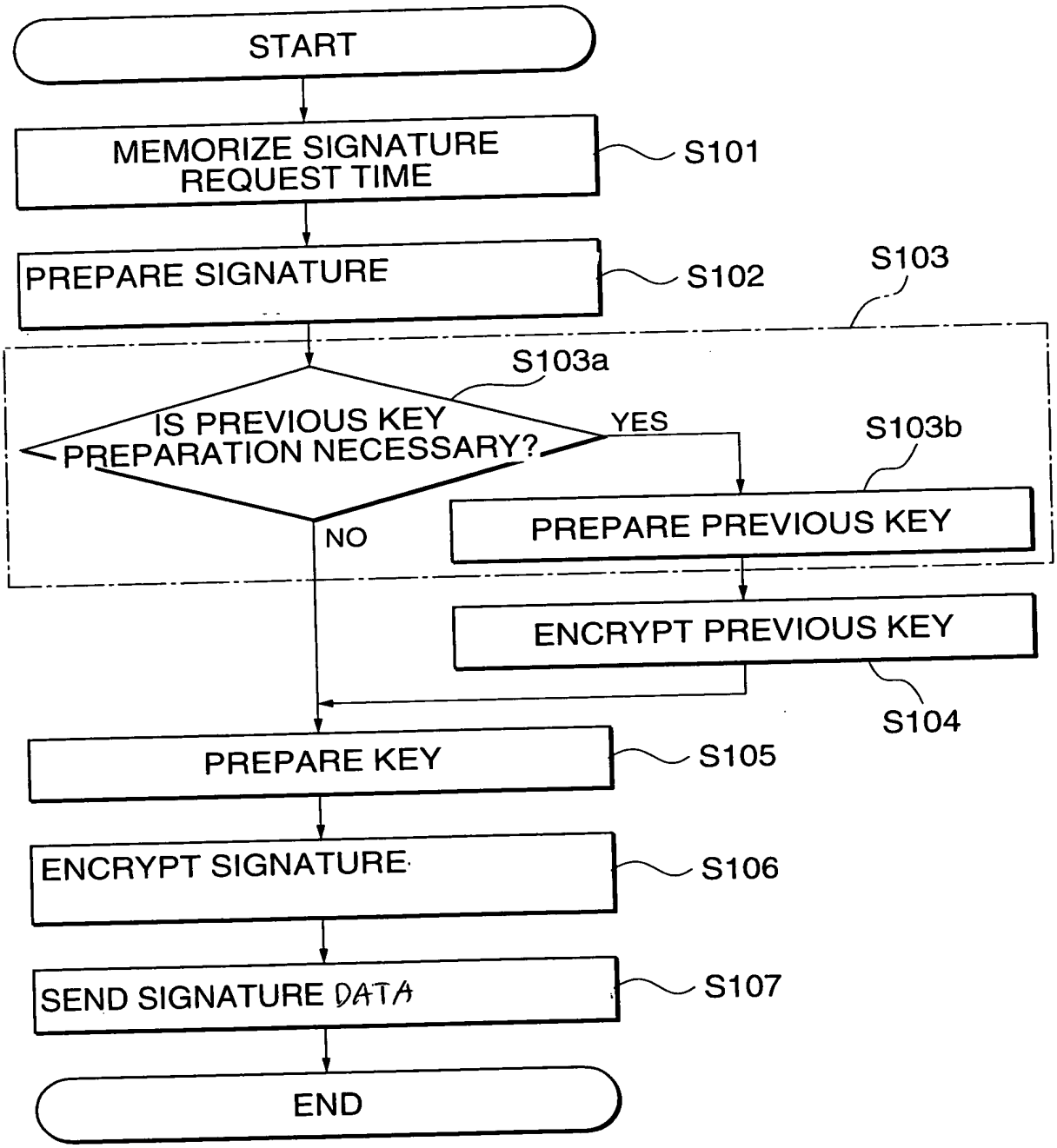

START
MEMORIZE SIGNATURE REQUEST TIME
S101
PREPARE SIGNATURE
S102
S103
S103a
IS PREVIOUS KEY PREPARATION NECESSARY?
YES
NO
S103b
PREPARE PREVIOUS KEY
ENCRYPT PREVIOUS KEY
S104
PREPARE KEY
S105
ENCRYPT SIGNATURE
S106
SEND SIGNATURE DATA
S107
END

FIG.3

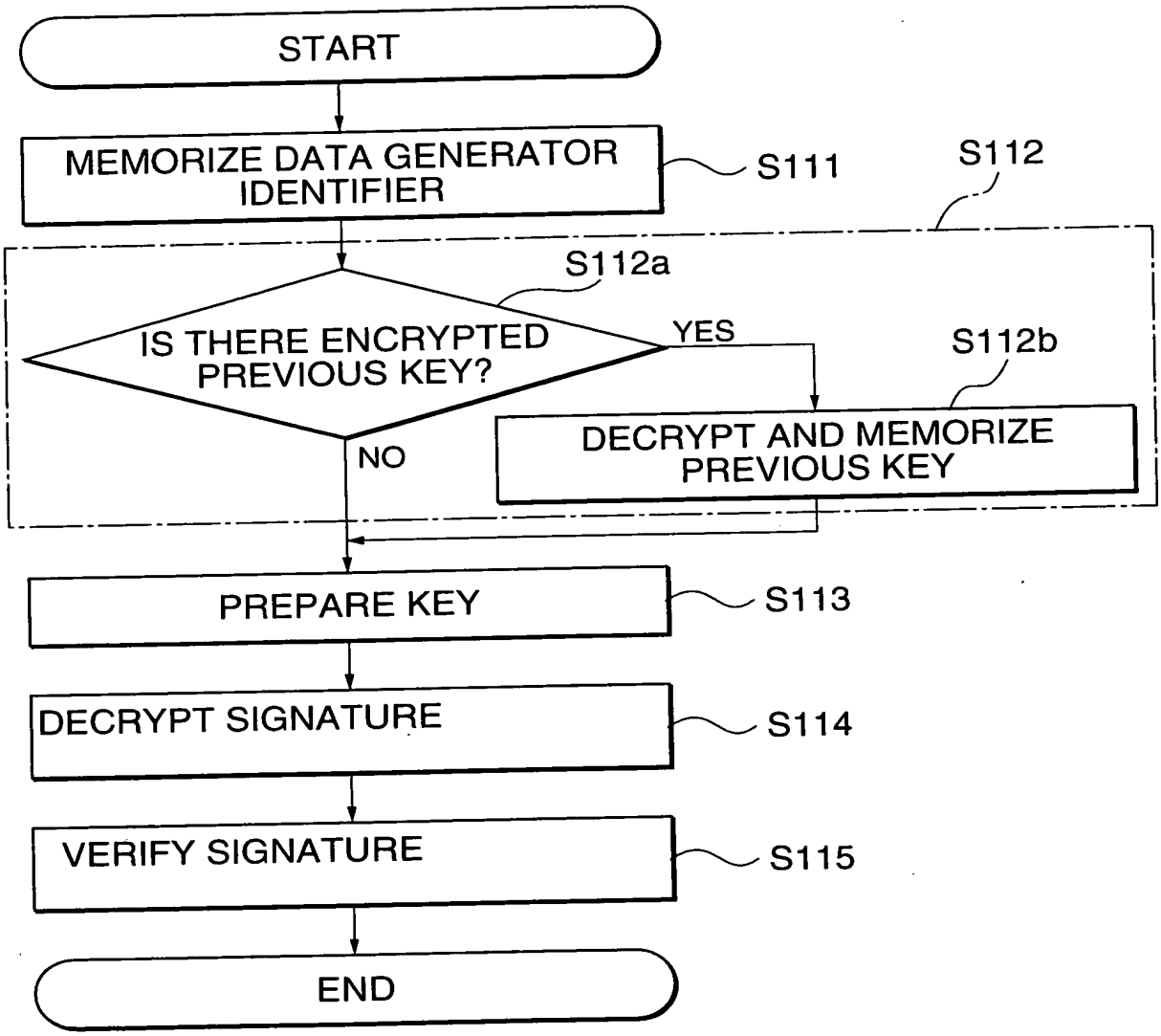

START
MEMORIZE DATA GENERATOR IDENTIFIER
S111
S112
S112a
IS THERE ENCRYPTED PREVIOUS KEY?
YES
S112b
DECRYPT AND MEMORIZE PREVIOUS KEY
NO
PREPARE KEY
S113
DECRYPT SIGNATURE
S114
VERIFY SIGNATURE
S115
END

FIG.4

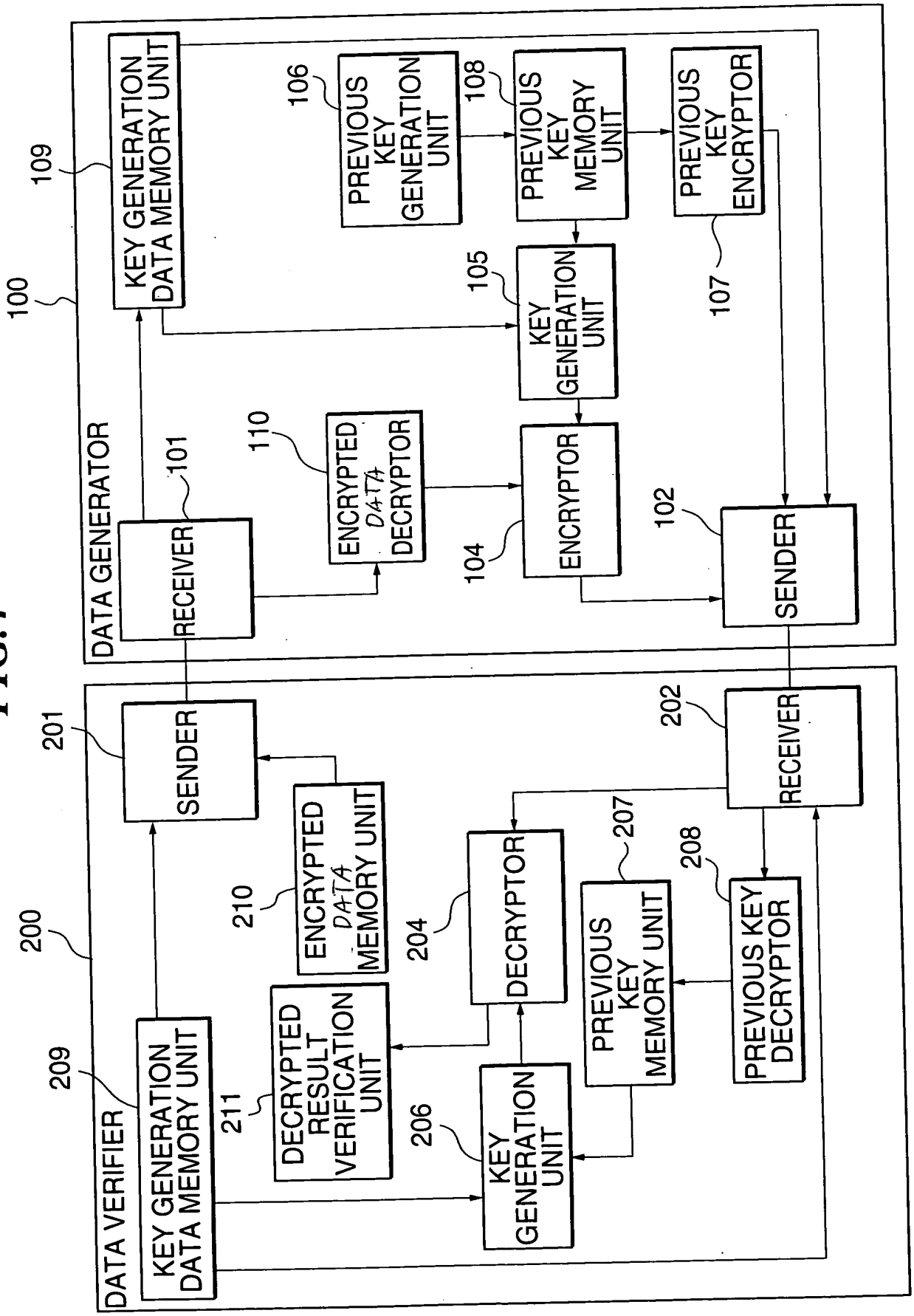

DATA GENERATOR
100
KEY GENERATION DATA MEMORY UNIT
109
PREVIOUS KEY GENERATION UNIT
106
PREVIOUS KEY MEMORY UNIT
108
PREVIOUS KEY ENCRYPTOR
107
KEY GENERATION UNIT
105
RECEIVER
101
ENCRYPTED DATA DECRYPTOR
110
ENCRYPTOR
104
SENDER
102
DATA VERIFIER
200
KEY GENERATION DATA MEMORY UNIT
209
SENDER
201
RECEIVER
202
ENCRYPTED DATA MEMORY UNIT
210
DECRYPTOR
204
DECRYPTED RESULT VERIFICATION UNIT
211
PREVIOUS KEY MEMORY UNIT
207
PREVIOUS KEY DECRYPTOR
208
KEY GENERATION UNIT
206

FIG.5

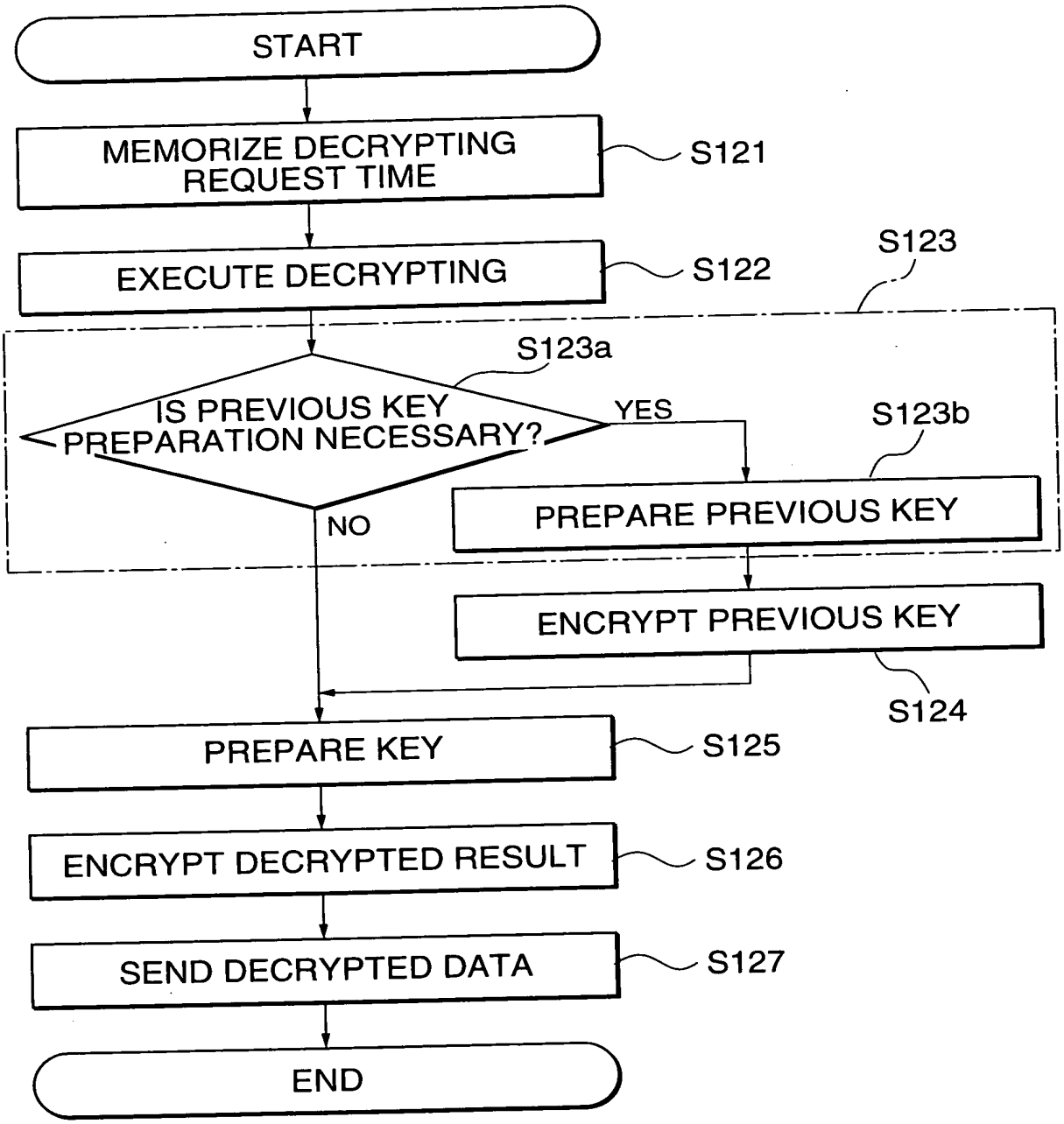

START
MEMORIZE DECRYPTING REQUEST TIME
S121
EXECUTE DECRYPTING
S122
S123
S123a
IS PREVIOUS KEY PREPARATION NECESSARY?
YES
NO
S123b
PREPARE PREVIOUS KEY
ENCRYPT PREVIOUS KEY
S124
PREPARE KEY
S125
ENCRYPT DECRYPTED RESULT
S126
SEND DECRYPTED DATA
S127
END

FIG.6

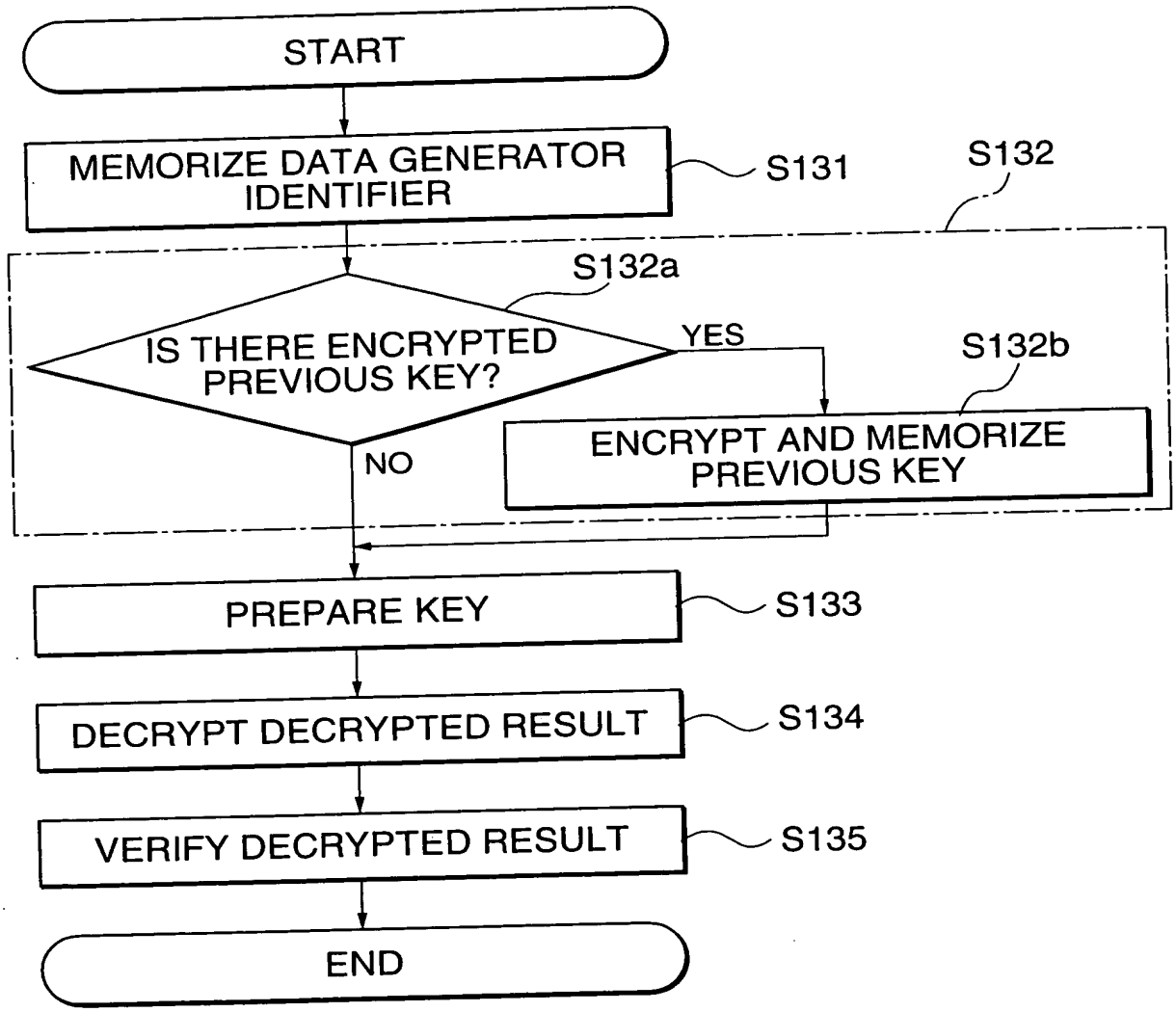

START
MEMORIZE DATA GENERATOR IDENTIFIER
S131
S132
S132a
IS THERE ENCRYPTED PREVIOUS KEY?
YES
NO
S132b
ENCRYPT AND MEMORIZE PREVIOUS KEY
PREPARE KEY
S133
DECRYPT DECRYPTED RESULT
S134
VERIFY DECRYPTED RESULT
S135
END

FIG.7

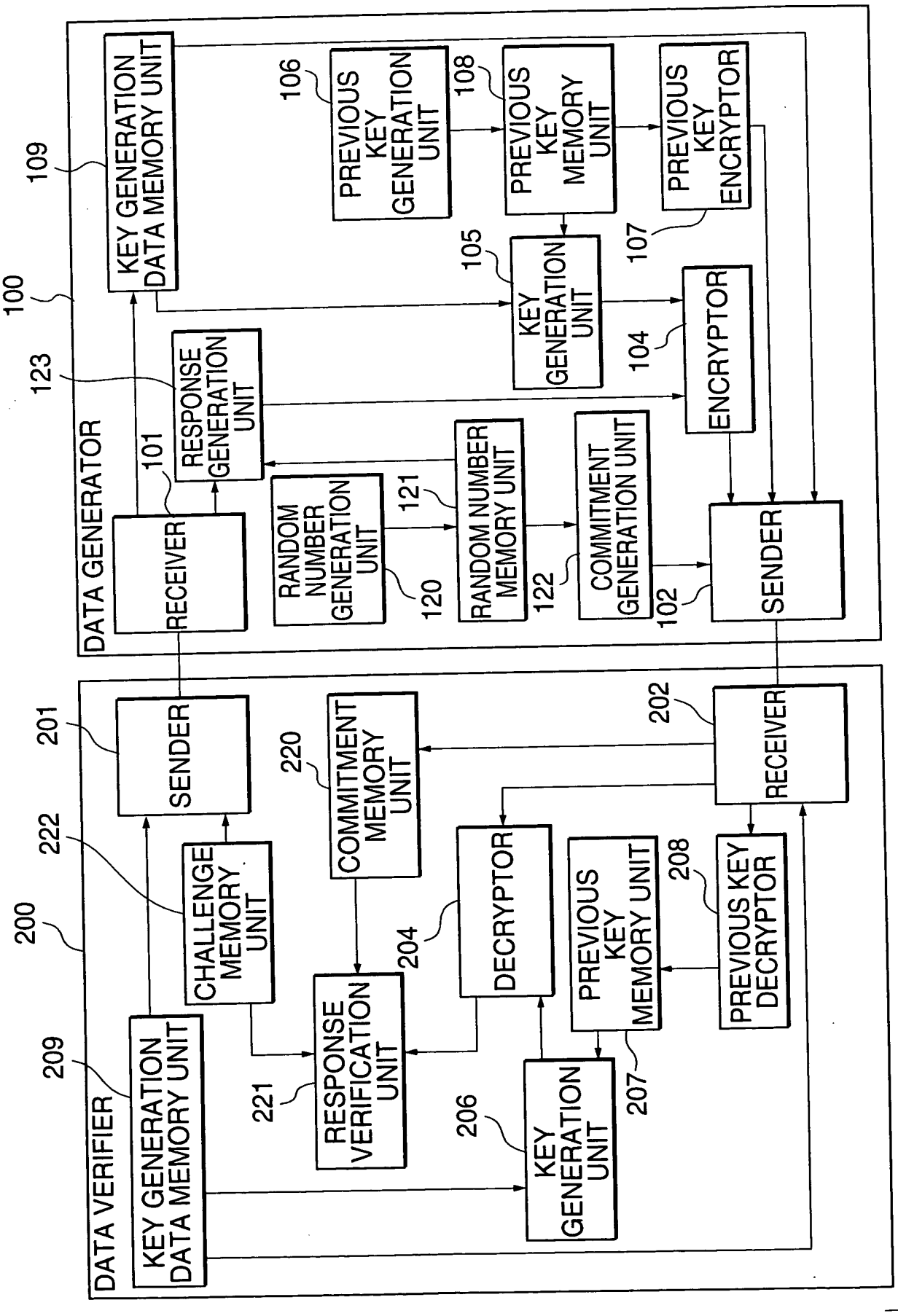

DATA GENERATOR
100
KEY GENERATION DATA MEMORY UNIT
109
PREVIOUS KEY GENERATION UNIT
106
PREVIOUS KEY MEMORY UNIT
108
PREVIOUS KEY ENCRYPTOR
107
KEY GENERATION UNIT
105
ENCRYPTOR
104
RESPONSE GENERATION UNIT
123
RECEIVER
101
RANDOM NUMBER GENERATION UNIT
120
RANDOM NUMBER MEMORY UNIT
121
COMMITMENT GENERATION UNIT
122
SENDER
102
DATA VERIFIER
200
SENDER
201
COMMITMENT MEMORY UNIT
220
RECEIVER
202
CHALLENGE MEMORY UNIT
222
DECRYPTOR
204
PREVIOUS KEY MEMORY UNIT
208
PREVIOUS KEY DECRYPTOR
KEY GENERATION DATA MEMORY UNIT
209
RESPONSE VERIFICATION UNIT
221
KEY GENERATION UNIT
206
207

FIG.8

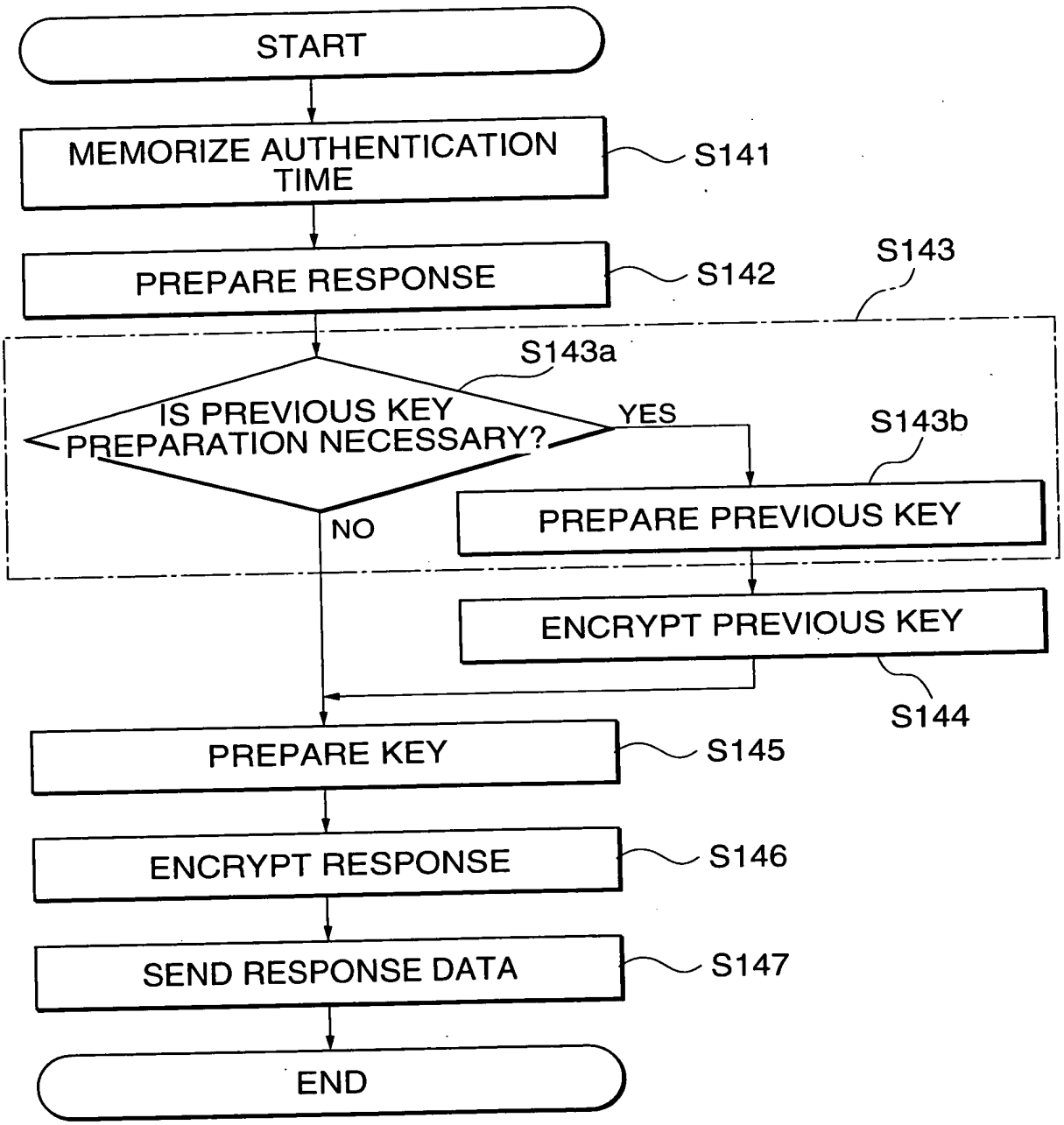

START
MEMORIZE AUTHENTICATION TIME
S141
PREPARE RESPONSE
S142
S143
S143a
IS PREVIOUS KEY PREPARATION NECESSARY?
YES
NO
S143b
PREPARE PREVIOUS KEY
ENCRYPT PREVIOUS KEY
S144
PREPARE KEY
S145
ENCRYPT RESPONSE
S146
SEND RESPONSE DATA
S147
END

FIG.9

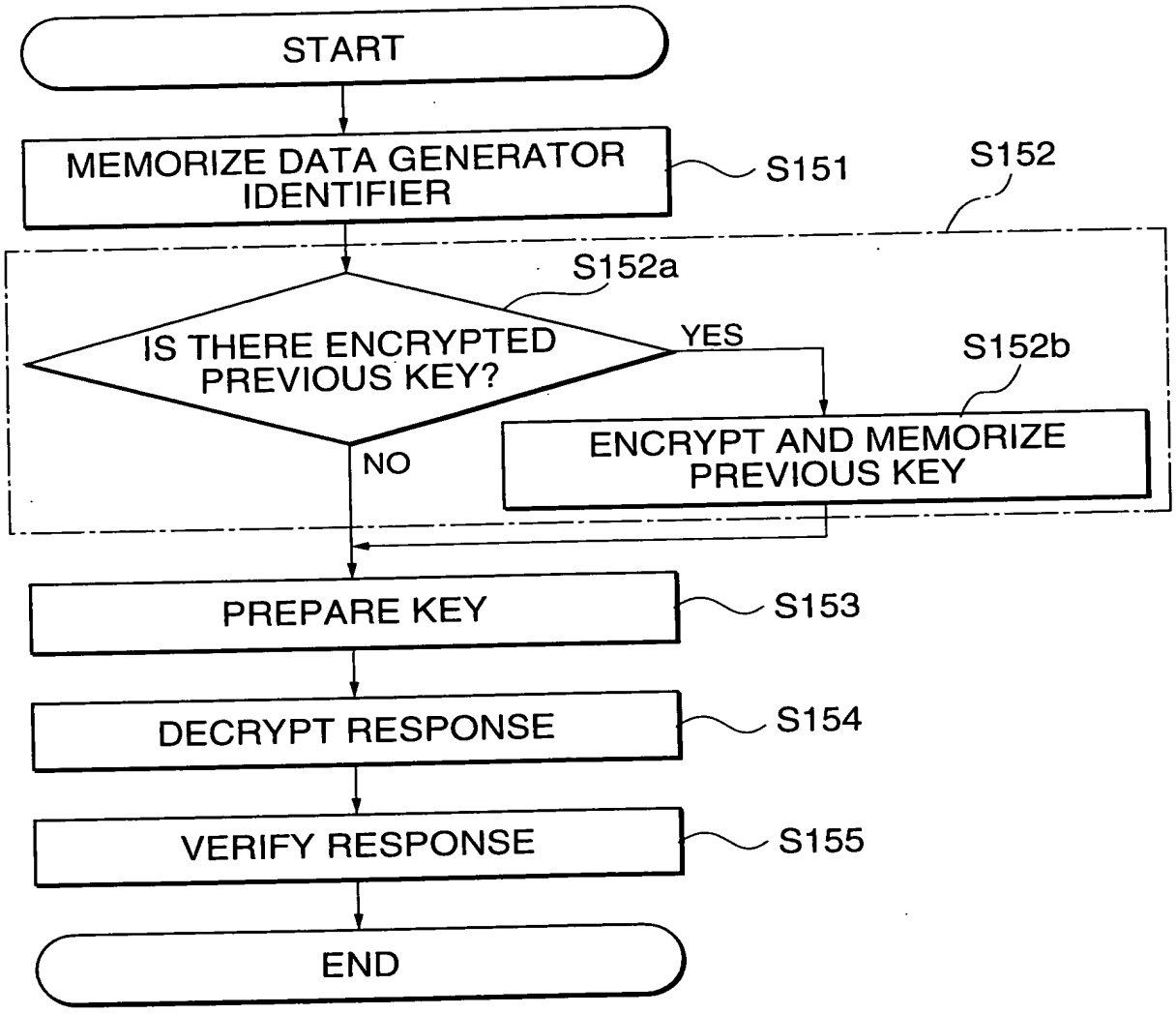
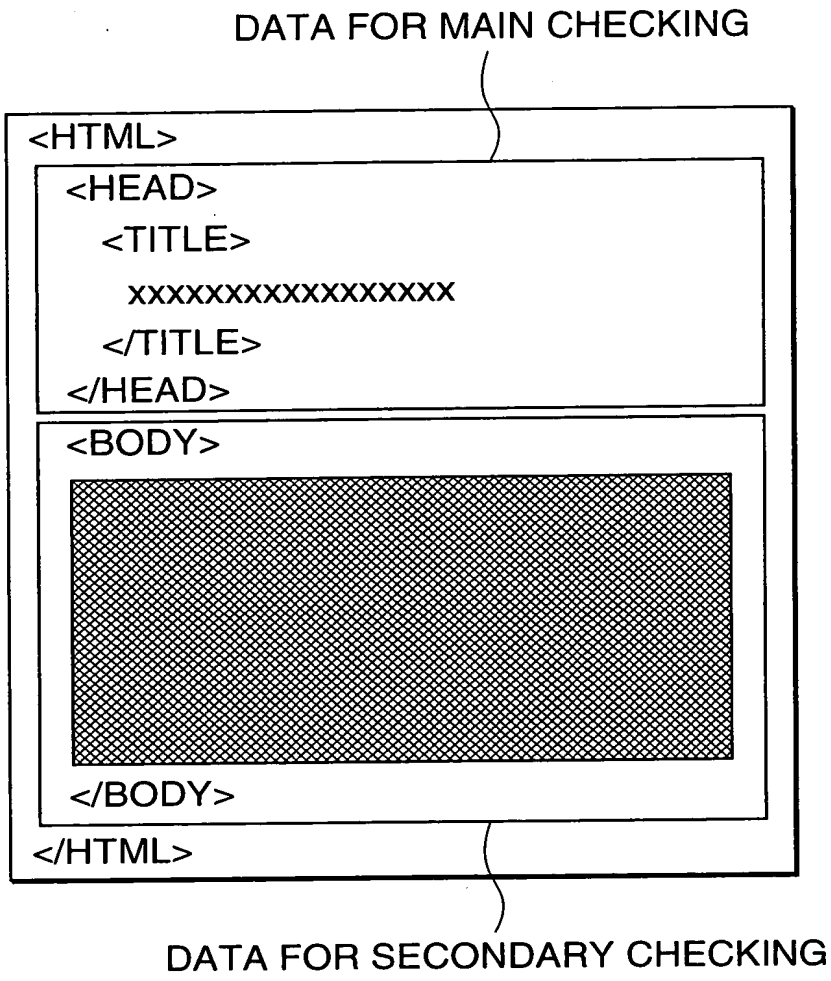

START
MEMORIZE DATA GENERATOR IDENTIFIER
S151
S152
S152a
IS THERE ENCRYPTED PREVIOUS KEY?
YES
NO
S152b
ENCRYPT AND MEMORIZE PREVIOUS KEY
PREPARE KEY
S153
DECRYPT RESPONSE
S154
VERIFY RESPONSE
S155
END

FIG.10


DATA FOR MAIN CHECKING
<HTML>
<HEAD>
<TITLE>
xxxxxxxxxxxxxxxx
</TITLE>
</HEAD>
<BODY>
</BODY>
</HTML>
DATA FOR SECONDARY CHECKING